東大和市情報セキュリティポリシー
(情報セキュリティ基本方針)

平成２８年４月１日

目　次

１．目的　・・・・・・・・・・・・・・・・・・・・　２
２．用語の定義　・・・・・・・・・・・・・・・・・　２
３．情報資産に対する脅威　・・・・・・・・・・・　３
４．適用範囲　・・・・・・・・・・・・・・・・・・　３
５．職員及び外部委託事業者等の遵守義務　・・　３
６．情報セキュリティ対策　・・・・・・・・・・　３
７．情報セキュリティ監査と自己点検の実施　・　４
８．情報セキュリティポリシーの見直し　・・・　４
９．情報セキュリティ対策基準及び
　　情報セキュリティ実施手順の策定　・・・・　４

東大和市情報セキュリティ基本方針

1　目的

市が保有する個人情報をはじめとする情報資産を、様々な脅威から守るとともに、行政サービスを安全かつ効率的に提供することにより、市政に対する市民からの信頼を高めることを目的として、情報セキュリティに係る基本的な事項を定める。

2　用語の定義

情報セキュリティ基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

（１）情報システム　サーバ（情報システムにおける基幹的・中核的なコンピュータをいう。以下、同じ。）、端末機等（職員が使用するパーソナルコンピュータ、周辺機器、記録媒体）、ネットワーク等で構成された情報処理を行う仕組みをいう。

（２）ネットワーク　サーバ、端末機等を相互に接続する通信回線、ルーター、ハブ等で構成された通信網をいう。

（３）情報資産　情報システム、ネットワーク、情報システムで取り扱う全ての情報（これらを印刷した文書を含む）及び情報システムの開発・運用に係る仕様書・手順書等の関連文書をいう。

（４）情報資産に対する脅威　①第三者による不正行為等の人的脅威、②地震災害等の物理的脅威、③データの改ざん、搾取等の技術的脅威等、情報資産の保護を脅かす要因をいう。

（５）情報セキュリティ　情報資産に係る機密性（許可された者だけが情報にアクセスできる状態を確保することをいう。）、完全性（情報が破壊、改ざん又は消去されていない状態を確保することをいう。）及び可用性（許可された者が必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。）を維持することをいう。

（６）サーバ室　市が保有する情報システムを運用するための本庁舎内の専用区画をいう。

（７）データセンター　市が保有する情報システムを運用するため、強固なセキュリティ対策が講じられた外部の専用施設をいう。

（８）執務室　職員が業務を行う区画又は部屋をいう。

（９）職員　市長部局及び各行政委員会に所属する全ての職員（再任用職員を含む）、嘱託員及び臨時職員をいう。

（１０）外部委託事業者等　市から情報システムの開発、運用、保守管理及び処理業務等を受託した者（再委託、再々委託等で受託した者も含む）、公の施設の指定管理者（地方自治法（昭和２２年法律第６７号）第２４４条の２第３項に規定する法人及びその他の団体）、派遣社員等をいう。

（１１）情報セキュリティポリシー　本基本方針及び情報セキュリティ対策基準（職員、外部委託事業者等が遵守すべき事項及び判断基準を定めたもの）の総称をいう。

（１２）情報システムマネジメント　情報化の推進、情報セキュリティの確保等、情報システムを適正に管理運営することをいう。

3　情報資産に対する脅威

情報資産に対する脅威は、次に掲げることを想定する。

（1）不正アクセス、不正プログラム（コンピュータウイルス、マルウェア等）の感染、標的型攻撃メール、サービス不能攻撃等のサイバー攻撃、部外者による侵入等、意図的な要因による情報資産の漏えい、搾取、破壊、改ざん、消去等

（2）職員又は外部委託事業者等による情報資産の無断持ち出し、無許可ソフトウェアの使用、無許可デバイスの使用等の内部不正行為による情報資産の漏えい、破壊、改ざん、消去等

（3）職員又は外部委託事業者等による非意図的な操作・設定ミス等に起因する漏えい、破壊、改ざん、消去等

（4）情報システムやネットワークの設計・開発の不備、プログラムの欠陥、保守・管理の不備によるシステム障害等

（5）地震、落雷等の自然災害及び火災等による行政サービスの停止

（6）大規模・広範囲に及ぶ伝染病等の発生（パンデミック等）による要員不足に伴うシステム運用の機能不全

（7）電力供給、情報通信の途絶等の重要インフラの障害からの波及

（8）その他情報セキュリティを脅かす事案

4　適用範囲

（1）市が保有する情報資産

（2）情報資産を取り扱う全ての職員及び外部委託事業者等

5　職員及び外部委託事業者等の遵守義務

職員及び外部委託事業者等は、業務の遂行にあたり、情報資産毎の重要性について共通認識を持ち、適切に情報資産を取り扱わなければならない。

また、本基本方針のほか、別に定める情報セキュリティ対策基準、課毎に定める情報セキュリティ実施手順、その他情報セキュリティを確保するために必要な法令等を遵守しなければならない。

6　情報セキュリティ対策

（1）組織体制の整備

適切な情報セキュリティ対策を実施するため、全庁的な組織体制を整備する。

（2）情報資産の分類と管理

情報資産の内容と重要度に応じて、別に定める「情報資産の分類」のとおり分類し、当該分類に基づき適切に管理する。

（３）人的セキュリティ対策

情報資産を取り扱う職員及び外部委託事業者等が遵守すべき事項を定めるとともに、十分な教育及び啓発等の人的な対策を講じる。

（４）物理的セキュリティ対策

サーバ室、データセンター、執務室に対する部外者の不正侵入、端末機の盗難防止等の物理的な対策を講じる。

（５）技術的セキュリティ対策

情報システムへの不正アクセスによる重要データの毀損、漏えい等を防止するためのアクセス制御及び不正プログラムの感染等を防止するための技術的な対策を講じる。

（６）運用面におけるセキュリティ対策

情報システム等の運用管理を外部委託する際は、情報システムの設計・開発の不備、設備の保守管理の不備等によるシステム障害が生じないよう、適切な対策を講じる。

また、情報システム等の運用における信頼性を高めるため、万が一の情報セキュリティインシデントに備えた即応体制を整えるとともに、大規模災害等に備えたバックアップ体制等を確立し、様々なシステム障害の発生に備えるため、緊急時対応計画を整備する。

７　情報セキュリティ監査と自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、東大和市保有個人情報管理規程（平成２７年１２月２２日訓令第２２号）第３２条、第３３条及び別に定める情報セキュリティ監査基準に基づき、情報セキュリティ監査及び自己点検等を実施する。

８　情報セキュリティ対策の見直し

情報セキュリティ監査及び自己点検等の結果、並びに情報セキュリティに関する情勢の変化等に対応するため、適宜、情報セキュリティ対策を見直す。

９　情報セキュリティ対策基準及び情報セキュリティ実施手順の策定

情報セキュリティ対策に関する遵守事項及び判断基準をまとめた対策基準を策定するとともに、より具体的な手順を定めた実施手順を策定する。

なお、情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることで市の行政運営及び情報セキュリティ確保に重大な支障を及ぼす恐れがあることから非公開とする。